Cisco IOS および Cisco Unified Communications Manager での音声の脆弱性

Critical

アドバイザリーID : cisco-sa-20070808-IOS-voice

初公開日 : 2007-08-08 16:00

バージョン 2.0 : Final

CVSSスコア : 10.0

回避策 : No Workarounds available

Cisco バグ ID : CSCeb21064 CSCse40276 CSCsb24007 CSCsf30058 CSCsi80749 CSCsf11855 CSCsd81407 CSCse05642 CSCsi60004 CSCsg70474 CSCsc60249 CSCsf08998 CSCse68355 CSCse68138

CVE-2007-4291 CVE-2007-4295 CVE-2007-4294 CVE-2007-4292

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco IOS ソフトウェアでは音声に関連する複数の脆弱性が発見されており、そのうちの 1 つは Cisco Unified Communications Manager にも該当します。 これらの脆弱性は、次のプロトコルまたは機能に関係しています。

- Session Initiation Protocol（SIP; セッション開始プロトコル）
- Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）
- シグナリング プロトコル H.323、H.254
- Real-Time Transport Protocol（RTP; リアルタイム転送プロトコル）
- ファックス受信

Cisco では、該当するお客様用に、これらの脆弱性に対応する無償ソフトウェアを提供しております。 「**ソフトウェア バージョンと修正**」セクションの一覧に記載されている修正済みの Cisco IOS ソフトウェアには、このアドバイザリで説明されているすべての脆弱性に対する修正が含まれています。

プロトコルまたは機能自体を無効にする以外に、この脆弱性の影響を緩和する回避策はありませ

ん。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice で掲示されます。

注: 2007 年 8 月 8 日に公開された情報には、4 つのセキュリティ アドバイザリと 1 つのセキュリティ レスポンスが含まれます。 それらのアドバイザリはすべて IOS に該当し、さらに 1 つは Cisco Unified Communications にも該当します。 各アドバイザリには、そのアドバイザリで説明されている脆弱性を修正したリリースが掲載されているだけでなく、4 つのアドバイザリで説明されているすべての脆弱性を修正したリリースに関する詳細も掲載されています。 各ドキュメントへのリンクは次のとおりです。

- IPv6 ルーティング ヘッダー使用による Cisco IOS の情報漏えい
  Pv6-leak
- Cisco IOS Next Hop Resolution Protocol の脆弱性
  808-nhrp
- Cisco IOS Secure Copy における認可バイパスの脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-scp
- Cisco IOS および Cisco Unified Communications Manager での音声の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice
- Cisco Unified MeetingPlace XSS の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070808-mp

該当製品

これらの脆弱性が該当するのは、Cisco IOS が稼働していて、音声サービスが有効になっているデバイスだけです。 Cisco Bug ID CSCsi80102Cisco Unified Communications Manager

脆弱性のある製品

Cisco IOS 製品で実行されているソフトウェアを確認するには、デバイスにログインし、**show version** コマンドを発行してシステム バナーを表示します。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力の次の行には、カッコに囲まれたイメージ名が表示され、その後にバージョンと Cisco IOS リリース名が続きます。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は、IOS イメージを実行しているデバイスからの出力例です。

```
Router>show version
Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 31-Mar-05 08:04 by yiyan
```

Cisco IOS ソフトウェア リリースの命名方法に関する詳細については、次のリンクを参照して

ください。 http://www.cisco.com/web/about/security/intelligence/ios-ref.html。

SIP 関連の脆弱性

脆弱なバージョンの IOS を実行し、SIP 処理をサポートしている Cisco デバイスには、脆弱性が存在する可能性があります。 これには、12.2、12.3、および 12.4 の複数の IOS バージョンが含まれます。 SIP Public Switched Telephone Network（PSTN; 公衆電話交換網）ゲートウェイおよび SIP Session Border Controller（SBC; セッション ボーダー コントローラ）として設定されているルータには、脆弱性があります。 CAT6000-CMM カードにも脆弱性が存在します。

特定のデバイスで SIP が有効になっているかどうかを確認するには、**show ip sockets** コマンドおよび **show tcp brief all** コマンドを入力します。 一部の新しい IOS リリースでは、**show ip sockets** コマンドが削除されています。 その場合は、**show udp** を使用してください。 出力は **show ip sockets** コマンドと同じです。

```
Router#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
17 0.0.0.0             0  --any--          5060   0   0  211   0
17 0.0.0.0             0 192.168.100.2       67   0   0 2211   0
17 0.0.0.0             0 192.168.100.2     2517   0   0   11   0
```

UDP SIP が有効であることは、UDP ポート 5060 を含む最初の行によって示されます。

```
Router#show tcp brief all
TCB       Local Address           Foreign Address        (state)
2051E680  *.5060                  *.*                    LISTEN
```

TCP SIP が有効であることは、*.5060 を含む行によって示されます。

SIP が明示的に設定されていない場合でも、デバイスには脆弱性が存在します。 **show ip sockets** コマンドの出力で、デバイスがポート 5060 をリスニングしていることが示されている場合、そのデバイスは脆弱です。

MGCP 関連の脆弱性

IOS デバイスで MGCP が設定されているかどうかを調べるには、Cisco IOS の設定に次のいずれかの行が含まれているかどうかを確認します。

```
Router#show running config
....
voice-port 1/1/1
!
mgcp
!
dial-peer voice 1 pots
 service mgcpapp
 port 1/1/1
```

または

```
Router#show running config
....
controller T1 1/1
 framing sf
 linecode ami
 pri-group timeslots 1-24 service mgcp
```

または

```
Router#show running config
....
controller T1 1/1
 framing sf
 linecode ami
 ds0-group 0 timeslots 1-24 type none service mgcp
```

実際のポート番号は、設定によって異なります。

H.323 シグナリング関連の脆弱性

IOS デバイスで H.323 が設定されているかどうかを調べるには、Cisco IOS の設定に次のいずれかの行が含まれているかどうかを確認します。

次の設定は、Cisco Bug ID CSCsi60004（登録ユーザ専用）に対して脆弱です。

```
Router#show running config | include proxy
proxy h323
```

次の設定は、Cisco Bug ID CSCsg70474（登録ユーザ専用）に対して 脆弱です。

```
Router#show running config | include inspect
ip inspect name H323_protocol h323
 ip inspect H323_protocol in
```

リアルタイム転送プロトコル関連の脆弱性

RTP はオーディオ情報またはビデオ情報が送信されるときに呼び出されるので、このプロトコルを有効にするために特別な設定を行う必要はありません。 ルータで RTP パケットを処理するためには、H.323、MGCP、SIP、または H.320 のいずれかのプロトコルによってパケットが処理されている必要があります。

注: これらの脆弱性はデバイス自体で終わるか、または起きるセッションだけにないトランジットトラフィック影響を与えます; たとえば、トラフィックはデバイスを通る、影響を受けていません他の所で送信されますが。

ファックス受信の脆弱性

Digital Signal Processor（DSP; デジタル信号プロセッサ）が存在する場合、IOS デバイスはフ

ァックス受信をデフォルトでリスニングします。 デバイスに DSP が存在するかどうかを調べるには、次のコマンドを実行します。

注: この脆弱性はデバイス自体で終わるか、または起きるセッションだけにないトランジットトラフィック影響を与えます; たとえば、トラフィックはデバイスを通る、影響を受けていません他の所で送信されますが。

```
Router#show voice dsp
 DSP   DSP             DSPWARE CURR   BOOT                          PAK     TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE    RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ============
C542 001 01 None       7.4.1 IDLE  idle      0  0 1/1/0     NA     0       598/607
C542 002 01 None       7.4.1 IDLE  idle      0  0 1/1/1     NA     0       591/588
```

この例は、デバイスに DSP が存在することを示しています。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。次のデバイスは該当しないことが確認されています。

- Cisco Unified Communications ManagerCSCsi80102
- Cisco IP Phone

詳細

これらの脆弱性の詳細は、カテゴリと影響によってグループ化されます。

SIP 関連の脆弱性

SIP は、マルチメディア セッションの確立、変更、および終了に使用されるプロトコルです。 多くの場合、SIP はインターネット電話で使用されます。 SIP のコール シグナリングでは、基礎になるトランスポート プロトコルとして、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）または Transport Control Protocol（TCP; 伝送制御プロトコル）を使用できます。 いずれの場合も、不正な形式の SIP パケットを処理することによって、脆弱性が発現する可能性があります。

不正な形式の SIP パケットを受信すると、脆弱なデバイスはクラッシュする場合があり、任意のコードが実行される可能性があります。 これらの脆弱性は次の Cisco Bug ID に記述されています。

- CSCsi80749：Crash while processing malformed SIP packet（登録ユーザ専用）
- CSCsi80102：CUCM - Crash while processing malformed SIP packet（登録ユーザ専用）

不正な形式の SIP パケットを受信すると、メモリ リークやデバイスのクラッシュが発生する可能性があります。 これらの脆弱性は次の Cisco Bug ID に記述されています。

- CSCsf11855：Crash while processing malformed SIP packet（登録ユーザ専用）
- CSCeb21064：Crash while processing malformed SIP packet（登録ユーザ専用）
- CSCse40276：Router crashed by malformed SIP message（登録ユーザ専用）
- CSCse68355：Router crashed by malformed SIP packet（登録ユーザ専用）
- CSCsf30058：Memory leak when processing malformed SIP message（登録ユーザ専用）
- CSCsb24007：Memory corruption and unexpected reload on receiving a SIP packet（登録ユーザ専用）
- CSCsc60249：Crash while processing malformed SIP packet（登録ユーザ専用）

MGCP 関連の脆弱性

MGCP は、メディア ゲートウェイ コントローラやコール エージェントなどの外部コール制御要素からメディア ゲートウェイを制御するためのプロトコルです。 通常、メディア ゲートウェイは、電話回線上を伝送されるオーディオ信号と、インターネットやその他のパケット ネットワーク上で伝送されるデータ パケットの間の変換を行うネットワーク要素です。 Cisco 環境の場合、メディア ゲートウェイは Cisco Communications Manager と Cisco ルータの間で使用され、音声ゲートウェイとして機能します。

特別に作成された MGCP パケットを受信すると、脆弱なデバイスがクラッシュしたり、応答不能になったりする可能性があります。 応答不能になったデバイスは、新しい電話コールを確立できず、通常の動作に戻すにはリブートが必要です。 これらの脆弱性は次の Cisco Bug ID に記述されています。

- CSCsf08998：MGCP stop responding after receiving malformed packet（登録ユーザ専用）
- CSCsd81407：Router crash on receiving abnormal MGCP messages（登録ユーザ専用）

H.323 シグナリング関連の脆弱性

H.323 は、IP を使用するネットワークでのマルチメディア通信とシグナリングに関する International Telecommunications Union（ITU）勧告です。

不正な形式の H.323 パケットを受信すると、脆弱なデバイスがクラッシュする可能性があります。 これらの脆弱性は次の Cisco Bug ID に記述されています。

- CSCsi60004H323 Proxy Unregistration from Gatekeeper
- CSCsg70474：IOS FW with h323 inspect crashes when malformed H.323 packets received（登録ユーザ専用）

リアルタイム転送プロトコル関連の脆弱性

RTP は、対話形式のオーディオやビデオなど、リアルタイムでのデータ配信サービスを提供するためのプロトコルです。

不正な形式の RTP パケットを受信すると、脆弱なデバイスがクラッシュする可能性があります。これらの脆弱性は次の Cisco Bug ID に記述されています。

- CSCse68138：Issue in handling specific packets in VOIP RTP Lib（登録ユーザ専用）

- CSCse05642：I/O memory corruption crash on a router（登録ユーザ専用）

ファックス受信の脆弱性

大きいパケットを受信すると、脆弱なデバイスがクラッシュする可能性があります。 この脆弱性は次の Cisco Bug ID に記述されています。

- CSCej20505：Router hangs with overly large packet（登録ユーザ専用）

回避策

このドキュメントで説明されている脆弱性に対する回避策はありません。 これらの脆弱性による影響を制限するために、いくつかの緩和策を適用することを推奨いたします。 その緩和策とは、適切なデバイスのみがルータに接続できるように設定することです。 その効果を高めるためには、緩和策とあわせて、ネットワーク エッジにアンチスプーフィング対策を適用する必要があります。 これらの脆弱性を含む音声プロトコルでは、トランスポート プロトコルとして UDP が使用される可能性があるため、この対処は必須です。

Cisco Unified Communications Manager では、このドキュメントで説明されているどの脆弱性も緩和できません。 すべての緩和策は、隣接するデバイスに適用する必要があります。

デバイスの通常動作に必要がない場合は、該当するプロトコルを無効にすることを推奨いたします。 ルータが SIP パケットを処理しないようにするには、次のコマンドを実行する必要があります。

```
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#end
```

注: MGCP コールまたは H.323 コールを処理しているデバイスにこの回避策を適用した場合、アクティブなコールが処理されている間は、SIP 処理を停止できません。 したがって、この回避策は、アクティブなコールを停止できるメンテナンス期間中に適用する必要があります。

Infrastructure Access Control List（iACL; インフラストラクチャ アクセス コントロール リスト）

ネットワークを通過するトラフィックをブロックすることは困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。 インフラストラクチャ ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。 次の示す ACL の例は、インフラストラクチャ IP アドレス範囲内の IP アドレスを持つすべてのデバイスを保護するために配備されたインフラストラクチャ アクセス リストの一部として含める必要があります。

Cisco IOS が稼働するデバイスのアクセス リストの例：

```
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#end
```

ホワイトペーパー 『Protecting Your Core: Infrastructure Protection Access Control Lists (ACL) には、インフラストラクチャ保護アクセス リストに関するガイドラインと推奨配備方法が記載されています。 このホワイトペーパーは、以下のリンクから入手可能です。 http://www.cisco.com/warp/public/707/iacl.html。

コントロール プレーン ポリシング

Control Plane Policing (CoPP; コントロール プレーン ポリシング) を使用すると、SIP (TCP および UDP ポート 5060 および 5061)、MGCP (UDP ポート 2427)、H.323 (TCP ポート 1720 と 11720 および UDP ポート 2517)、および RTP (UDP ポート 16384 ~ 32767) による、デバイスへの信頼できないアクセスをブロックできます。 Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。 デバイスに CoPP を設定して管理プレーンおよびコントロール プレーンを保護すると、インフラストラクチャへの直接攻撃のリスクと有効性を最小限に抑えることができます。 CoPP は、既存のセキュリティ ポリシーおよび設定に従ってインフラストラクチャ デバイス宛ての適正なトラフィックのみを明示的に許可することにより、管理プレーンとコントロール プレーンを保護します。 次の例では、192.168.100.1 が信頼できるホストになります。この例は、ネットワークに実際に適用できます。

```
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#end
```

上の CoPP の例には、悪用の可能性があるパケットと一致する「許可」アクションの Access Control List Entry (ACE; アクセス コントロール リスト エントリ) があるので、policy-map の「drop」機能によって悪用パケットは廃棄されます。 一方、(この例には示されていない)「deny」アクションに一致するパケットは、policy-map drop 機能の影響を受けません。

Cisco IOS トレイン 12.2S および 12.0S では、ポリシーマップの構文が異なることに注意してください。

```
Router(config)#sip-ua
Router(config-sip-ua)#no transport udp
Router(config-sip-ua)#no transport tcp
Router(config-sip-ua)#end
```

CoPP 機能の設定および使用のその他の情報は http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html および

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html で見つけることができます。

Cisco 機器に適用可能な追加の軽減策については以下の "Cisco Applied Intelligence companion document" より入手可能です。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20070808-IOS-voice

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

Cisco IOS のビルド方法、番号付け方法、管理方法についての詳細は、次の URL を参照してください。 http://www.cisco.com/web/about/security/intelligence/ios-ref.html

メジャー リリース	修正済みリリースの入手可能性	
該当する 12.0 ベースのリリース	First Fixed Release（修正された最初のリリース）	推奨リリース
12.0	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0DA	脆弱性なし	
12.0DB	脆弱性なし	
12.0DC	脆弱性なし	
12.0S	脆弱性なし	
12.0SC	脆弱性なし	

12.0SL	脆弱性なし	
12.0SP	脆弱性なし	
12.0ST	脆弱性なし	
12.0SX	脆弱性なし	
12.0SY	脆弱性なし	
12.0SZ	脆弱性なし	
12.0T	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0W	脆弱性なし	
12.0WC	12.0(5)WC16	
12.0WT	脆弱性なし	
12.0XA	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XB	脆弱性なし	
12.0XC	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XD	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XE	脆弱性あり; first fixed in 12.1(27b)E2	
12.0XF	脆弱性あり; contact TAC	
12.0XG	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XH	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XI	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XJ	脆弱性なし	
12.0XK	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XL	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XM	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XN	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)

12.0XQ	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XR	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XS	脆弱性なし	
12.0XV	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.0XW	脆弱性なし	
該当する 12.1 ベースのリリース	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.1	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1AA	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1AX	脆弱性なし	
12.1AY	脆弱性なし	
12.1AZ	脆弱性なし	
12.1CX	脆弱性なし	
12.1DA	脆弱性なし	
12.1DB	脆弱性なし	
12.1DC	脆弱性なし	
12.1E	12.1(27b)E2	
12.1EA	12.1(22)EA10	12.1(22)EA10a 12.1(22)EA10b; 利用可能 な 13-Sept-07
12.1EB	脆弱性なし	
12.1EC	脆弱性あり; first fixed in 12.2(4)BC1	12.3(17b)BC8 12.3(21a)BC3
12.1EO	脆弱性なし	
12.1EU	脆弱性なし	
12.1EV	脆弱性なし	
12.1EW	脆弱性なし	
12.1EX	脆弱性あり; first fixed in 12.1(27b)E2	
12.1EY	脆弱性あり; first fixed in 12.1(27b)E2	
12.1EZ	脆弱性あり; first fixed in 12.1(27b)E2	

12.1GA	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1GB	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1T	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XA	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XB	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XC	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XD	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XE	脆弱性あり; first fixed in 12.1(27b)E2	
12.1XF	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XG	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XH	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XI	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-	12.2(46a)

	Aug-07	
12.1XJ	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XK	脆弱性なし	
12.1XL	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XM	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XN	脆弱性なし	
12.1XO	脆弱性なし	
12.1XP	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XQ	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b)

		12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XR	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XS	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XT	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XU	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1XV	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07

		12.3(17c); 利用可能 な 16-Aug-07
12.1XW	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XX	脆弱性なし	
12.1XY	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1XZ	脆弱性あり; first fixed in 12.2(26c); 利用可能 な 14-Aug-07	12.2(46a)
12.1YA	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YB	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YC	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YD	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a)

		12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YE	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YF	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YG	脆弱性なし	
12.1YH	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.1YI	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07

12.1YJ	脆弱性なし	
該当する 12.2 ベースのリリース	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.2	12.2(26c); 利用可能 な 14-Aug-07 12.2(27c); 利用可能 な 14-Aug-07 12.2(28d); 利用可能 な 14-Aug-07 12.2(29b); 利用可能 な 14-Aug-07 12.2(46a); 利用可能 な 15-Aug-07	12.2(46a)
12.2B	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2BC	脆弱性なし	
12.2BW	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2BY	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
12.2CY	脆弱性なし	

12.2CZ	脆弱性あり; contact TAC	
12.2DA	脆弱性なし	
12.2DD	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2DX	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2EU	脆弱性なし	
12.2EW	脆弱性なし	
12.2EWA	脆弱性なし	
12.2EX	脆弱性なし	
12.2EY	脆弱性なし	
12.2EZ	脆弱性なし	
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性なし	
12.2IXA	脆弱性あり; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXB	脆弱性あり; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXC	脆弱性あり; first fixed in 12.2(18)IXD1	12.2(18)IXD1
12.2IXD	12.2(18)IXD1	12.2(18)IXD1
12.2IXE	脆弱性なし	
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性なし	
12.2MC	12.2(15)MC1 12.2(15)MC2a 12.2(15)MC2i 12.2(8)MC1 12.2(8)MC2	12.2(15)MC2j

12.2S	12.2(14)S19 12.2(18)S13 12.2(20)S13 12.2(25)S13 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2SB	12.2(28)SB1 12.2(31)SB6	12.2(28)SB9; 利用可能 な 15-Aug-07 12.2(31)SB6
12.2SBC	脆弱性あり; first fixed in 12.2(28)SB1	12.2(28)SB9; 利用可能 な 15-Aug-07 12.2(31)SB6
12.2SE	脆弱性なし	
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性なし	
12.2SED	脆弱性なし	
12.2SEE	脆弱性なし	
12.2SEF	脆弱性なし	
12.2SEG	脆弱性なし	
12.2SG	脆弱性なし	
12.2SGA	脆弱性なし	
12.2SL	脆弱性なし	
12.2SM	脆弱性なし	
12.2SO	脆弱性なし	
12.2SRA	12.2(33)SRA5	12.2(33)SRA5
12.2SRB	12.2(33)SRB2; 利用可能 な 31-Aug-07	12.2(33)SRB2; 利用可能 な 31-Aug-07
12.2SU	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2SV	12.2(22)SV 12.2(23)SV 12.2(24)SV 12.2(25)SV 12.2(27)SV2 12.2(27)SV3 12.2(28)SV1 12.2(29)SV	12.2(29)SV4; 利用可能 な 14-Oct-07

	12.2(29a)SV	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性あり; contact TAC	
12.2SW	12.2(20)SW 12.2(21)SW 12.2(21)SW1 12.2(25)SW10 12.2(25)SW11	12.2(25)SW11
12.2SX	脆弱性あり; first fixed in 12.2(18)SXF10	
12.2SXA	脆弱性あり; first fixed in 12.2(18)SXF10	
12.2SXB	脆弱性あり; first fixed in 12.2(18)SXF10	12.2(18)SXF10
12.2SXD	脆弱性あり; contact TAC	
12.2SXE	脆弱性あり; first fixed in 12.2(18)SXF10	12.2(18)SXF10
12.2SXF	12.2(18)SXF10	12.2(18)SXF10
12.2SXH	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性あり; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2T	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能な 16-Aug-07 12.3(17c); 利用可能な 16-Aug-07
12.2TPC	12.2(8)TPC10c; 利用可能な 17-Aug-07	12.2(8)TPC10c
12.2UZ	脆弱性なし	
12.2VZ	脆弱性あり; first fixed in 12.2(31)SB6	12.2(28)SB9; 利用可能な 15-Aug-07 12.2(31)SB6
12.2XA	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能な 16-Aug-07

		12.3(17c); 利用可能 な 16-Aug-07
12.2XB	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XC	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2XD	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XE	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XF	脆弱性なし	
12.2XG	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a)

		12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XH	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XI	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XJ	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XK	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XL	脆弱性あり; first fixed in	12.3(23)

	12.3(23)	12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XM	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XN	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XQ	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XR	脆弱性なし	
12.2XS	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07

		12.3(17c); 利用可能 な 16-Aug-07
12.2XT	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XU	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XV	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2XW	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YA	12.2(4)YA12; 利用可能 な 17-Aug-07	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a)

		12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YB	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YC	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YD	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YE	脆弱性あり; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2YF	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07

12.2YG	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YH	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YJ	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YK	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YL	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c)

		12.4(13d)
12.2YM	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YN	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YO	脆弱性なし	
12.2YP	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YQ	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YR	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16)

		12.4(10c) 12.4(13d)
12.2YS	脆弱性あり; contact TAC	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YT	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2YU	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YV	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YW	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c)

		12.4(13d)
12.2YX	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YY	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2YZ	脆弱性あり; first fixed in 12.2(30)S	12.2(25)S13 12.2(14)S19
12.2ZA	脆弱性なし	
12.2ZB	12.2(8)ZB	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZC	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZD	脆弱性あり; contact TAC	
12.2ZE	脆弱性あり; first fixed in 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利

		用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.2ZF	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZG	脆弱性あり; contact TAC	12.3(2)XA6 12.3(8)YG6; 利用可能 な 16-Aug-07
12.2ZH	12.2(13)ZH9; 利用可能 な 17-Aug-07	12.2(13)ZH9
12.2ZJ	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZL	、first fixed in 12.3(11)T12 脆弱、Cisco 17xx のための 利用可能 な 16-Aug-07; Cisco 3200 については 12.4(16) で初めて修正 12.3(7)XR7 で初めて修正 （ICS7750 用は 2007 年 8 月 13 日に入手可能）	
12.2ZP	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.2ZR	脆弱性あり; contact TAC	
12.2ZU	脆弱性あり; first fixed in	12.2(33)SXH;

	12.2(33)SXH; 利用可能 な 31-Aug-07	利用可能 な 31-Aug-07
12.2ZW	脆弱性あり; contact TAC	
12.2ZY	12.2(18)ZY1	12.2(18)ZY2; 利用可能 な 14-Sep-07
該当する 12.3 ベースのリリース	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.3	12.3(17c); 利用可能 な 16-Aug-07 12.3(18a); 利用可能 な 16-Aug-07 12.3(19a); 利用可能 な 16-Aug-07 12.3(20a) 12.3(21b) 12.3(22a) 12.3(23)	12.3(23) 12.3(20a) 12.3(21b) 12.3(22a) 12.3(18a) 12.3(19a); 利用可能 な 16-Aug-07 12.3(17c); 利用可能 な 16-Aug-07
12.3B	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3BC	脆弱性なし	
12.3BW	脆弱性なし	
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	
12.3JEB	脆弱性なし	
12.3JK	脆弱性なし	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	一部のプラットフォームをサポート 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c)

		12.4(13d)
12.3TPC	12.3(4)TPC11b; 利用可能 な 17-Aug-07	12.3(4)TPC11b; 利用可能 な 17-Aug-07
12.3VA	脆弱性なし	
12.3XA	12.3(2)XA6	12.3(2)XA6
12.3XB	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XC	12.3(2)XC5	12.3(2)XC5
12.3XD	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XE	12.3(2)XE5; 利用可能 な 17-Aug-07	12.3(2)XE5
12.3XF	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XG	脆弱性あり; contact TAC	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XH	脆弱性あり; first fixed in	12.4(12c)

	12.3(11)T12; 利用可能 な 16-Aug-07	12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XI	12.3(7)XI1b 12.3(7)XI8a 12.3(7)XI2a	12.3(7)XI10a; 利用可能 な 21-Aug-07
12.3XJ	脆弱性あり; first fixed in 12.3(14)YX9; 利用可能 な 13-Aug-07	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3XK	脆弱性あり; first fixed in 12.3(11)T12; 利用可能 な 16-Aug-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XQ	脆弱性あり; first fixed in 12.4(16)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XR	12.3(7)XR7; 利用可能 な 17-Aug-07	12.3(7)XR7; 利用可能 な 17-Aug-07
12.3XS	脆弱性あり; first fixed in 12.4(16)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.3XU	12.3(8)XU	12.4(11)T3 12.4(9)T5; 利用可能 な 24-

		Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3XW	脆弱性あり; first fixed in 12.3(14)YX9; 利用可能 な 13-Aug-07	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3XY	脆弱性あり; contact TAC	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YA	脆弱性あり; first fixed in 12.4(16)	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d) 12.3(8)YG6; 利用可能 な 16-Aug-07
12.3YD	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YF	脆弱性あり; first fixed in 12.3(14)YX9; 利用可能 な 13-Aug-07	12.3(14)YX9; 利用可能 な 13-Aug-07

12.3YG	12.3(8)YG6; 利用可能 な 16-Aug-07	12.3(8)YG6; 利用可能 な 16-Aug-07
12.3YH	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YI	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YJ	脆弱性なし	
12.3YK	12.3(11)YK3; 利用可能 な 20-Aug-07	12.3(11)YK3; 利用可能 な 20-Aug-07
12.3YM	12.3(14)YM11; 利用可能 な 23-Aug-07	12.3(14)YM11; 利用可能 な 23-Aug-07
12.3YQ	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YS	脆弱性あり; first fixed in 12.4(11)T3	12.3(11)YS2
12.3YT	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-

		Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.3YU	脆弱性あり; first fixed in 12.4(2)XB6; 利用可能 な 16-Aug-07	12.4(2)XB6; 利用可能 な 16-Aug-07
12.3YX	12.3(14)YX9; 利用可能 な 13-Aug-07	12.3(14)YX9; 利用可能 な 13-Aug-07
12.3YZ	12.3(11)YZ2; 利用可能 な 17-Aug-07	12.3(11)YZ2; 利用可能 な 17-Aug-07
該当する 12.4 ベースのリリース	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**
12.4	12.4(10c); 利用可能 な 20-Aug-07 12.4(12c) 12.4(13d) 12.4(16) 12.4(3h); 利用可能 な 20-Aug-07 12.4(5c); 利用可能 な 15-Aug-07 12.4(7f) 12.4(8d); 利用可能 な 3-Sep-07	12.4(12c) 12.4(3h) 12.4(5c) 12.4(8d); 利用可能 な 03-Sep-07 12.4(7f) 12.4(16) 12.4(10c) 12.4(13d)
12.4JA	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	12.4(12)MR2; 利用可能 な 14-Aug-07	12.4(12)MR2
12.4SW	脆弱性なし	
12.4T	12.4(11)T3 12.4(15)T1 12.4(2)T6; 利用可能 な 3-Sep-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(9)T5; 利用可能 な 24-Aug-07	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07

		12.4(6)T8 12.4(15)T1
12.4XA	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.4XB	12.4(2)XB6; 利用可能 な 16-Aug-07	12.4(2)XB6; 利用可能 な 16-Aug-07
12.4XC	12.4(4)XC7; 利用可能 な 17-Aug-07	12.4(4)XC7
12.4XD	12.4(4)XD8; 利用可能 な 13-Aug-07	12.4(4)XD8; 利用可能 な 30-Aug-07
12.4XE	12.4(6)XE3; 利用可能 な 17-Aug-07	12.4(6)XE3
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	12.4(11)XJ4	12.4(11)XJ4
12.4XK	脆弱性あり; first fixed in 12.4(11)T3	12.4(11)T3 12.4(9)T5; 利用可能 な 24-Aug-07 12.4(2)T6; 利用可能 な 20-Aug-07 12.4(4)T8; 利用可能 な 28-Aug-07 12.4(6)T8 12.4(15)T1
12.4XT	12.4(6)XT1; 利用可能 な 17-Aug-07	12.4(6)XT1
12.4XV	12.4(11)XV1; 利用可能 な 17-Aug-07	12.4(11)XV1
12.4XW	12.4(11)XW2 12.4(11)XW3; 利用可能 な 24-Aug-07	12.4(11)XW3; 利用可能 な 13-Aug-07

Cisco Unified Communications Manager の修正済みソフトウェア

CUCM バージョン	修正済みリリース	ダウンロード場所
CUCM 3.3	Not affected	ソフトウェア リリース 3.3 は、CSCsi80102（登録ユーザ専用）には該当しません。
CUCM 4.x	Not affected	4.x のソフトウェア リリースはいずれも、CSCsi80102（登録ユーザ専用）には該当しません。
CUCM 5.0	未提供	CUCM 5.1(2b) へのアップグレード
CUCM 5.1	5.1(2b)	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-51?psrtdcat20e2
CUCM 6.0	6.0(1a)	http://www.cisco.com/pcgi-bin/tablebuild.pl/callmgr-60

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

次の脆弱性は、社内テストで発見されたものです。

- CSCsi80749：Crash while processing malformed SIP packet
- CSCsi80102：CUCM - Crash while processing malformed SIP packet
- CSCeb21064：Crash while processing malformed SIP packet
- CSCse40276：Router crashed by malformed SIP message
- CSCse68355：Router crashed by malformed SIP packet
- CSCsf30058：Memory leak when processing malformed SIP message
- CSCsf08998：MGCP stop responding after receiving malformed packet
- CSCsd81407：Router crash on receiving abnormal MGCP messages
- CSCsg70474：IOS FW with h323 inspect crashes when malformed H.323 packets received
- CSCse68138：Issue in handling specific packets in VOIP RTP Lib

次の脆弱性は、お客様のネットワークで発見されたものです。

- CSCsf11855：Crash while processing malformed SIP packet
- CSCsb24007：Memory corruption and unexpected reload on receiving a SIP packet
- CSCsc60249：Crash while processing malformed SIP packet
- CSCsi60004：H323 Proxy Unregistration from Gatekeeper
- CSCse05642：I/O memory corruption crash on a router
- CSCej20505：Router hangs with overly large packet

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice

改訂履歴

リビジョン 1.2	2007 年 8 月 20 日	「脆弱性を含む製品」セクションの SIP 関連の脆弱性を更新。
リビジョン 1.1	2007 年 8 月 8 日	「Infrastructure Access Control List (iACL; インフラストラクチャ アクセス コントロール リスト) 」セクションのコマンドを更新。
リビジョン 1.0	2007 年 8 月 8 日	初回公開リリース

利用規約